



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:  
David E. MCDYSAN et al.

Application No.: 09/723,481

Group Art Unit: 2155

Filed: November 28, 2000

Examiner: Bates, K.

Customer No.: 25537  
Attorney Docket: RIC00042  
Client Docket: 09710-1232

For: PROGRAMMABLE ACCESS DEVICE FOR A DISTRIBUTED NETWORK ACCESS SYSTEM

## APPEAL BRIEF

Honorable Commissioner for Patents  
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed June 19, 2006.

## **I. REAL PARTY IN INTEREST**

Verizon is the real party in interest.

## II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals and interferences.

03/02 2005 AVIATION 00000002 03723481  
14 074500Z 000.00 CP

**III. STATUS OF THE CLAIMS**

Claims 1-14, 16-38, and 40-50 are pending in this appeal, claims 15 and 39 having been canceled. No claim is allowed. This appeal is therefore taken from the final rejection of claims 1-14, 16-38, and 40-50 on February 9, 2006.

**IV. STATUS OF AMENDMENTS**

No amendment to claims has been filed after final rejection.

**V. SUMMARY OF CLAIMED SUBJECT MATTER**

The present claimed invention addresses problems associated with a network access system. More particularly, the present claimed invention relates to an IP-based communication network including a network access system having distributed and separate routing, signaling, service control, filtering, policy control and other functionality from IP forwarding. (*See, e.g.*, specification, p. 1, lines 25-29)

Conventional monolithic router designs have limited flexibility and extensibility. The present claimed invention recognizes that it would be desirable, in view of the rapid growth of Internet traffic, to dynamically provision, configure, and/or reallocate access capacity to IP-based services. Because access capacity is necessarily limited and providing additional access capacity is a major cost component of networks, the enforcement of intelligent admission control policies and provision of differing qualities of service is vital to the efficient utilization of available access capacity. However, conventional edge routers are not capable of classifying a wide variety of traffic types while enforcing policy controls or of responding to dynamic requests for capacity, and this functionality is difficult to incorporate within currently deployed monolithic edge routers. The present claimed invention accordingly recognizes that it would be desirable to

provide the above as well as additional policy control, network monitoring, diagnostic, and security services in commercialized hardware, while permitting these services to be tailored to meet the needs of individual customers and service providers. (See, e.g., specification, p. 3, line 29 - p. 4, line 14)

A distributed network access system architecture including a programmable access device is introduced. The programmable access device includes first and second network interfaces through which packets are communicated with a network, a forwarding table utilized to route packets communicated between the first and second network interfaces, and a packet header filter. (See, e.g., independent claims 1 and 26) The packet header filter identifies messages received at one of the first and second network interfaces on which policy-based services are to be implemented and passes identified messages via a message interface to an external processor for processing. (See, e.g., independent claims 1, 26, and 50, *see, also, e.g.,* claim 19 and specification, p. 41, line 5 - p. 45, line 8, FIGs. 9A-9E; claim 20 and specification, p. 46, line 4 - p. 47, line 29, FIGs. 10A-10C; and specification, p. 48, line 27 - p. 49, line 25, FIGs. 10G-10H) The packet header filter may be capable of filtering packets for service processing based upon protocol information pertaining to protocol layers higher than layer 3. The programmable access device may also include a usage monitor that reports events, such as session activity levels, to the external processor, a policer that polices packets by reference to programmed traffic parameters (*see, e.g.,* independent claim 50), and a scheduler that schedules the transmission of outgoing packets to support multiple quality of service classes.

In addition to the programmable access device, the distributed network access system architecture may include an external processor and an access router. Thus, conventional, proprietary edge routers are replaced with a distributed network access system that allocates the

functionality of traditional edge routers (as well as additional functionality) among three logical modules: a programmable access device, an external processor, and an access router. Basic routing of packets between input and output ports of the access network is performed by the access router. However, forwarding and generic traffic conditioning functions, such as marking, policing, monitoring, shaping, and filtering, are implemented in the programmable access device (*see, e.g.*, independent claim 50), and service functions, such as message interpretation, signaling, admission control, and policy invocation, are implemented in the external processor (*see, e.g.*, independent claims 1 and 26). (*See, e.g.*, specification, p. 5, lines 3 - 32)

More specifically, for example, a communication network 30 includes one or more core communication links 38 (e.g., trunk lines) coupled to one or more core routers 36. However, in contrast to conventional communication networks, such as that illustrated in Figure 1, customer router 32 does not interface to communication network 30 via a monolithic, proprietary edge router. Instead, customer equipment, such as customer router 32, interfaces with communication 30 via a network access system 31 that distributes the functions of traditional edge routers (as well as additional functionality) among three logical modules: a programmable access device (PAD) 40, an external processor 42, and an access router 44. Basic routing of packets between input and output ports of the access network is performed by access router 44 by reference to forwarding table 50 as determined by Exterior Gateway Protocol (EGP) and Interior Gateway Protocol (IGP) routing tables 52 and 54. However, forwarding and generic traffic conditioning functions, such as marking, policing, monitoring, shaping, and filtering, are implemented in programmable access device 40 (*see, e.g.*, independent claim 50), and service functions, such as message interpretation, signaling, admission control, and policy invocation, are implemented in external processor 42 (*see, e.g.*, independent claims 1 and 26). Given this distribution of

functionality, incoming and outgoing packets are typically communicated between core communication links 38 and customer router 32 via programmable access device 40, access router 44, and core router 36 (and optionally additional switching the access network, such as an Asynchronous Transfer Mode (ATM) or Multiprotocol Label Switching (MPLS) switch 60).

If filtering functionality of the programmable access device (PAD) 40 detects packet flows for which services, additional to typical services afforded by the configuration to incoming and outgoing packets are appropriate, the programmable access device 40 passes appropriate messages to the external processor 42 (*See, e.g.*, independent claims 1 and 26) for service processing via a Message, Control, and Reporting Interface (MCRI) 58 (*See, e.g.*, independent claim 50), which can be accessed via an Application Programming Interface (API) on the programmable access device 40 and external processor 42. Distributing functionality between access router 44, programmable access device 40 and external processor 42 in this manner gives the service provider (or even third parties) the freedom to extend and modify existing services, create new services, or add more processing power to external processor 42 without adversely affecting the forwarding performance of the programmable access device 40 and the routing performance or functionality of access router 44. This distribution of functionality results in numerous advantages, including improved scalability, flexibility, extensibility, interoperability, security, and service provisioning.

To implement a desired functionality for programmable access device 40 and external processor 42, the service provider (or even a customer or third party) can define policy rules in the policy database 46 of one or more servers 48 (also referred to as a policy decision point (PDP)). Policy server 48 then makes policy decisions that control the functionality and operation of programmable access device 40 and external processors 42 by reference to the policy rules

stored in policy database 46. Policy server 48 communicates policy decisions and associated configuration parameters for external processor 42 via a Service Policy Interface (SPI) 56, which can be accessed, for example, via an application program interface (API) on policy server 48 and external processor 42. Communication via Service Policy Interface 56 can employ any of a number of policy query protocols, including Common Open Policy Service (COPS) and Lightweight Directory Access Protocol (LDAP), which are respectively defined by Internet Engineering Task Force (IETF) RFCs 2748 and 2251. External processor 42 relays configuration parameters for programmable access device 40, if any, to programmable access device 40 via Message, Control, and Reporting Interface 58. (*See, e.g.*, specification, p. 10, line 14 - p. 11, line 31, FIGs. 2, 4)

Generally speaking, the functional modules of programmable access device 40 are logically arranged in incoming (e.g., from customer router 32) and outgoing (e.g., to customer router 32) traffic paths, with the incoming path including packet header filter 80, marker/policer 82, monitor(s) 84, forwarding table 86, and output buffers and scheduler 88. The outgoing path similarly includes packet header filter 90, forwarding table 86, monitor(s) 92, marker/shaper 94, and output buffers and scheduler 96. The functions of all of these functional modules can be independently configured or programmed by an external processor 42 through Message, Control, and Reporting Interface 58. (*See, e.g.*, independent claims 1, 26, and 50)

Incoming packets received from customer router 34 at the external interface of programmable access device 40 are first processed by packet header filter 80, which distinguishes between various message types using any one or a combination of the protocol type, Source Address (SA), Destination Address (DA), Type Of Service (TOS), Diffserv Codepoint (DSCP), Source Port (SP), Destination Port (DP), and other fields of a packet (e.g., layer 4 and higher

layer fields such as the SYN, ACK, RST, and FIN TCP flags) upon which packet header filter 80 is configured to filter. In addition to filtering on layer-3 information, packet header filter 80 has the ability to identify higher layer (i.e., layer 4-7) message types or specific fields and forward those messages from/to external processor 42 based on the configured filter parameters. Thus, based upon its filter configuration and the fields of an incoming packet, packet header filter 80 directs the packet either to an external processor 42 via message interface 100 or to a specific marker/policer 82 (see, e.g., independent claims 1, 26, and 50). Message interface 100 may also inject a packet specified by external processor 42 into either of packet header filters 80 and 90. (See, e.g., specification, p. 13, lines 7-32, FIGs. 2, 3)

In response to a stream of packets from packet header filter 80, marker/policer 82 polices the packet stream by applying one or more token or leaky bucket algorithms to determine whether the packet stream conforms to the traffic parameters established by control interface 104. As a result of the policing function, marker/policer 82 may discard nonconforming packets, mark nonconforming packets (e.g., with a higher or lower priority), and/or count nonconforming packets, depending upon its configuration (See, e.g., independent claim 50). If marking is required, marker/policer 82 may set bits in the Differentiated Services (DiffServ)/TOS byte in the IP packet header, and/or the 3-bit Multiprotocol Label Switching (MPLS) experimental field, and/or the 20-bit MPLS label field, and/or other fields as configured by control interface 104 for that particular packet stream.

Within the incoming path, one or more monitors 84 having different functions may be included. For example, these monitors 84 may include a usage monitor that tracks statistics for different layer-2, layer-3, layer-4, and higher layer traffic types (e.g., to monitor a Service Level Agreement (SLA)). Monitors 84 may also include a fault/troubleshooting/debugging monitor

(*see, e.g.*, dependent claim 11) that verifies conformance to standards to standards and assists in code debugging and fault diagnosis by saving and reporting memory dumps and other related information to external processor 42 via reporting interface 102 and Message, Control, and Reporting Interface 58. To regulate reporting messages, thresholds and other criteria can be set up to invoke a reporting event. The reporting messages sent to external processor 42 by monitors 84 may summarize usage information for a particular customer, report the occurrence of a high-priority traffic flow, alert external processor 42 to a large volume of out-of-band traffic, report on inactivity of a monitored flow, etc.

After processing by packet header filter 80, incoming packets are processed by forwarding table 86 (*see, e.g.*, independent claims 1 and 26). Forwarding table 86 maintains entries for each forwarding path, where each forwarding path is represented by packet flow attributes, such as DA, SA, TOS, PT, SP, DP, the incoming port, and the corresponding output port to which programmable access device 40 forwards the packet through the access network toward access router 44. Utilizing these forwarding table entries, forwarding table 86 forwards packets to the appropriate output ports and passes the packets to output buffers and scheduler 88. Output buffers and scheduler 88 buffer packets ready for transmission over communication network 30 and schedule the transmission of such packets. (*See, e.g.*, specification, page 14, line 1 - page 15, line 9, FIGs. 2, 3)

The outgoing path through programmable access device 40 is similar to the incoming path, except for the inclusion of marker/shaper 94 in lieu of marker/policer 82 (*see, e.g.*, independent claim 50). Marker/shaper 94 discards nonconforming packets, sends marked packets to appropriate output buffers for the various queues serving different QoS classes for individual flows within output buffers and scheduler 96 to control the delay, jitter and loss of an outgoing

packet flow, or simply counts non-conforming packets. (See, e.g., specification, page 15, lines 24-30, FIGs. 2, 3)

The external processor 42 performs at least three types of processing: invoking policy services, signaling to setup and teardown access network connections, and configuring one or more associated programmable access devices 40. To coordinate these different processing functions, external processor 42 contains one or more service controllers 120, which each may control these three functions for a respective type of service. For example, service controllers 120 may include any or all of a Conference Call Service Controller (CCSC), an E-Commerce Service Controller (ECSC), an IP Telephony Service Controller (IPTELSC), a Reserved Bandwidth Service Controller (RBSC), and a Multicast Service Controller (MSC). Each service controller may maintain a session table recording all of its active sessions with a programmable access device 40.

As further shown in FIG. 4, external processor 42 includes, for each associated programmable access device 40, a respective programmable access device controller 124. Under the direction of service controller(s) 120, each programmable access device controller 124 configures forwarding table 86, packet header filters 80 and 90, marker/policer 82, marker/shaper 94, monitors 84 and 92, and output buffers and schedulers 88 and 96 of the associated programmable access device 40 by invoking commands or scripts understood by control interface 104. External processor 42 also contains a respective message processor 122 for each associated programmable access device 40. Message processors 122 each communicate messages to and from the message interface 100 of the associated programmable access device 40. Upon receipt of a message from a programmable access device 40, which is usually a message received from the customer router 32, a message processor 122 parses the message and informs the appropriate

service controller (as determined by the type of service) of its contents. (See, e.g., specification, page 17, lines 4-31, FIGs. 3, 4)

Upon receipt of a report message from a reporting processor 126 or another message type from a message processor 122 included in the external processor 42, a service controller 120 of the external processor translates the message into one or more policy queries and transmits the policy query or queries to a policy server 48 via a Service Policy Interface (SPI) 56. A service controller 120 may also pass a message to another service controller 120 to obtain additional services via an interface 121.

In response to receipt of a policy decision from policy server 48, service controller 120 may inject one or more packets into a traffic flow via message processor 122, configure a programmable access device 40 via programmable access device controller 124 or control signaling inside or outside communication network 30 via signaling controllers 128a and 128b. Signaling controllers 128 support signaling protocols (e.g., Resource ReSerVation Protocol RSVP, Label Distribution Protocol (LDP), Private Network-Network Interface (PNNI), frame relay or ATM User Network Interface (UNI), etc.) to setup or tear down a Virtual Connection (VC) or Label Switched Path (LSP) across the network. A VC or LSP setup by a signaling controller 128 may have a specified Quality of Service (QoS). (See, e.g., specification, page 18, lines 13-31, FIGs. 2, 4, *see, also, e.g.*, specification, p. 29, line 20 - p. 30, line 27)

In summary, a distributed network access system consistent with features of the present invention replaces a monolithic edge router with a programmable access device containing at least filtering and forwarding functionality, an external processor having one or more service-specific controllers that implement policy-based control of the programmable access device, and an access router that performs basic routing. This distributed architecture has numerous benefits

over conventional monolithic router architectures, including scalability flexibility, extensibility, interoperability, security, and service provisioning. (See, e.g., specification, page 49, line 29 - page 50, line 5)

## **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Whether claims 1-2, 4-10, 16-17, 22-25, 26-27, 29-35, 40-41 and 46-49 are anticipated under 35 U.S.C. § 102 by *Alles et al.* (US 6,466,976)?

Whether claims 3, 28, and 50 are obvious over *Alles et al.* in view of *Amara et al.* (US 6,674,743)?

Whether claims 11 and 36 are obvious over *Alles et al.* in view of *Natarajan et al.* (US 6,505,244)?

Whether claims 12-14, 18, 37-38, and 42 are obvious over *Alles et al.* in view of *Gai et al.* (US 6,167,445)?

Whether claims 19-21 and 43-45 are obvious under 35 U.S.C. § 103 based on *Alles et al.* in view of Official Notice?

## **VII. ARGUMENT**

### **A. CLAIMS 1-2, 4-10, 16-17, 22-25, 26-27, 29-35, 40-41, AND 46-49 ARE NOT ANTICIPATED OVER ALLES ET AL.**

---

To anticipate a patent claim, every element and limitation of the claimed invention must be found in a single prior art reference, arranged as in the claim. *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383, 58 USPQ2d 1286, 1291 (Fed. Cir. 2001); *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 1576, 18 USPQ2d 1001, 1010 (Fed. Cir. 1991).

A prior art reference anticipates a patent claims if it discloses every limitation of the claimed invention, either explicitly or inherently. *In re Schreiber*, 128 F.3d 1473, 1477, 44 USPQ2d 1429, 1431 (Fed. Cir. 1997). “Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes, the claimed limitations, it anticipates.” *MEHL/Biophile Int'l Corp. v. Milgram*, 192 F.3d 1362, 1365, 52 USPQ2d 1303, 1305 (Fed. Cir. 1999).

#### 1. Claims 1-2, 4-10, 16-17, 22-25, 26-27, 29-35, 40-41 and 46-49

Independent claim 1 recites a “a packet header filter and a **forwarding table**, wherein the **forwarding table** is utilized to forward packets between the first and second interfaces . . . ; and a control interface through which said packet header filter and said **forwarding table** are programmed.” As for independent claim 26, that claim recites “routing packets by reference to a **forwarding table**” and “programming the packet header filter and the **forwarding table** through a control interface.” *Alles et al.*, however, lacks disclosure of the recited “forwarding table.”

Rather, *Alles et al.* is concerned with a system and method for providing desired services policies to subscribers accessing the Internet, which with the desired service policies are translated into processing rules. These processing rules contain an action and a classifier that “generally identifies the application data flows to which the action may be applied to provide the desired service polices for each subscriber” (Abstract). *Alles et al.* further explains that “[a]ll flows for a subscriber may be dedicated for initial processing by one of the processor groups. When ATM cells are used as data bit groups, the channel identifiers can be used for assignment to individual processor group” (col. 3:26-29). Details of the employment of the channel identifiers are given in a passage heavily cited by the Examiner as follows:

To determine the appropriate packet service card, switch fabric **340** may maintain a channel identifier associated with each channel on which the bit groups are received. In case of ATM cells, the VCI/VPI information in the bit groups uniquely defines such a channel. The physical port number (on which the data is received) and channel identifier may uniquely identify each subscriber (or a group of subscribers with non-overlapping IP addresses) when data is directly received from a subscriber and destined for the Internet. On the other hand, when data is received from the Internet, the determination of the associated subscriber may require examination of the IP header. In general, switch fabric **340** may buffer the cells until a last cell of a packet is received, and forwards all the cells for the packet to a packet service card allocated for an individual subscriber. . . .

Packet service card **350** may process the received cells according to processing rules to provide the desired service policies to each specific subscriber. Packet service card **350** first assembles the cell data into packets which can be identified with flow used in classifiers, and applies the processing rules. In the process, packet service card **350** determines whether to discard or forward the packet. The IP destination address may also be changed if transparent forwarding is a requested service for that system. (col. 10:36-50, 57-65)

In place, however, does *Alles et al.* describe the use of a “forwarding table.” In fact, the only occurrence of the word “table” in *Alles et al.* is in the caption of FIG. 5 in reference to a graphical chart. Although the Examiner’s final Office Action of Feb. 9, 2006, cites col. 10:59-65 for the clause, “wherein the **forwarding table** is utilized to forward packets between the first and second interfaces,” this passage is just about forwarding packets with no disclosure of the requisite forwarding table.

Acknowledging the factual inadequacy of *Alles et al.* for the recited “forwarding table” element, the Examiner contends in the Advisory Action of May 16, 2006, that “the switching fibre operates as both the forwarding table and packet filter.” The problem with the Examiner’s contention is that claim 1 is rejected under 35 U.S.C. § 102. Just as a disclosure of glue does not anticipate VELCRO™ even though they may arguably have similar fastening functions, neither does the disclosure of a different structure in *Alles et al.* anticipate claim 1’s different and specifically recited structure of a “forwarding table.”

Nor would such a “forwarding table” be inherent in *Alles et al.* Inherency requires the missing descriptive matter to be necessarily present in the reference, but this has not been shown by the Examiner. In fact, claim 1 further recites a specific type of forwarding table: one that can be programmed through a control interface. Thus, in order to salvage the 102 rejection, the Examiner would have to make the case that not merely a generic forwarding table—but a specific forwarding table programmable through a control interface—must be inherent in the descriptive matter missing from *Alles et al.*

Pursuant to 35 U.S.C. § 112, ¶ 4, dependent claims 2, 4-10, 16-17, 22-25, 27, 29-35, 40-41 and 46-49 incorporate all the features, elements, and limitations of their parent claims. Accordingly, these dependent claims are not anticipated by *Alles et al.*

## 2. Dependent Claims 4 and 29

Dependent claim 4 recites “wherein the packet header filter filters packets for service processing based upon protocol information pertaining to protocol layers higher than layer 3.” This feature too is lacking from *Alles et al.*

As described above, the *Alles et al.* system uses ATM channel numbers or the physical port number for routing. Indeed, the *Alles et al.* system predetermines which ATM cells are to be applied certain policies based on the subscriber identifier (col. 10:33-35). Instead of filtering based upon protocol information pertaining to protocol layers higher than layer 3, switch fabric 340 merely routes traffic based on a channel identifier to a corresponding specific packet service card 350, which applies the policy corresponding to the subscriber. Different channel identifiers are pre-designated to the corresponding packet service cards 350, without any need to filter, but routing to the packet service 350. In a sense, the determination of whether to apply any policy in the *Alles et al.*

*al.* system is performed in advance of the call arriving at the switch fabric 340, and therefore is not performed at the switch fabric 340.

However, ATM channel numbers and physical port numbers used for routing by the switch fabric 340 are protocol information merely at layers 3 and below, not “higher than layer 3,” as dependent claims 4 and 29 set forth.

**B. CLAIMS 3, 11-14, 18-21, 28, 36-38, 42-45, AND 50 ARE NOT OBVIOUS**

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention under any statutory provision always rests upon the Examiner. *In re Mayne*, 104 F.3d 1339, 41 USPQ2d 1451 (Fed. Cir. 1997); *In re Deuel*, 51 F.3d 1552, 34 USPQ2d 1210 (Fed. Cir. 1995); *In re Bell*, 991 F.2d 781, 26 USPQ2d 1529 (Fed. Cir. 1993); *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In rejecting a claim under 35 U.S.C. § 103, the Examiner is required to provide a factual basis to support the obviousness conclusion. *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967); *In re Lunsford*, 357 F.2d 385, 148 USPQ 721 (CCPA 1966); *In re Freed*, 425 F.2d 785, 165 USPQ 570 (CCPA 1970).

**1. Claims 19-21 and 43-45 are not obvious over *Alles et al.* and “Official Notice”**

The obviousness rejection of claims 19-21 and 43-45 over *Alles et al.* and “official notice” is improper and should be reversed. On page 6 of the final Office Action, the Examiner “takes Official Notice (see MPEP § 2144.03) that ‘the message protocol between the message identifier and external processors could be SIP, IGMP, or RSVP because they are simple, well-known communication protocols between many independent nodes in a network (Column 9, lines 53-58) in a computer networking environment was well known in the art at the time the invention was made.’”

However, the Administrative Procedures Act (APA) mandates the Patent Office to make the necessary findings and provide *an administrative record* showing the evidence on which the findings are based, accompanied by the reasoning in reaching its conclusions. See *In re Zurko*, 258 F.3d 1379, 1386, 59 USPQ2d 1693, 1697 (Fed. Cir. 2001); *In re Gartside*, 203 F.3d 1305, 1314, 53 USPQ2d 1769, 1774 (Fed. Cir. 2000). In particular, the Patent Office must articulate and place on the record the “common knowledge” used to negate patentability. *In re Zurko*, *id.*; *In re Lee*, 277 F.3d 1338, 1344-45, 61 USPQ2d 1430, 1434-35 (Fed. Cir. 2002).

The Examiner’s invocation of Official Notice is both unnecessary and improper. It is unnecessary because the existence of the SIP, IGMP, or RSVP protocols have already been made of record during the examination of the present application when the Examiner had cited the references of *Gibson et al.* (US 6,680,943) and *Jorgensen* (US 6,452,915).

The Examiner’s invocation of Official Notice is also improper because it attempts to take Official Notice, not of facts (for which the citations of *Gibson et al.* and *Jorgensen* should have sufficed) but of a legal conclusion of obviousness, thereby dispensing with the evidentiary requirement to show some teaching or motivation. Obviousness rejections require some evidence in the prior art of a teaching, motivation, or suggestion to combine and modify the prior art references. See, e.g., *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1351-52, 60 USPQ2d 1001, 1008 (Fed. Cir. 2001); *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25, 56 USPQ2d 1456, 1459 (Fed. Cir. 2000); *In re Dembicza*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999). The Patent Office must give specific reasons why one of ordinary skill in the art would have been motivated to combine the references. See, e.g., *In re Kotzab*, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000); *In re Rouffet*, 149 F.3d 1350, 1359, 47 USPQ2d 1453, 1459 (Fed. Cir. 1998).

Moreover, if the proposed modification or combination of the prior art would change the principle of operation of the reference being modified, then the teachings of the reference are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 813 123 USPQ 349, 352 (CCPA 1959). As explained in § VII. A. 2 above, the *Alles et al.* switch fabric 340 operates at protocol layers 3 and below, but the recited protocols SIP, IGMP, and RSVP are all above those layers. Thus, there is no way to alter the switch fabric 340, which relies on physical port numbers or channel identifiers to forward traffic, to parse ATM cells to view the entire data payload just to be able to detect such higher layer messaging of SIP, IGMP, or RSVP without necessitating a significant change in the principle of operation of the *Alles et al.* system.

### **2. Claims 12-14, 18, 37-38, and 42 are non-obvious over *Alles et al.* and *Gai et al.***

The obviousness rejection of claims 12-14, 18, 37-38, and 42 over *Alles et al.* and *Gai et al.* should also be reversed. *Gai et al.* is applied merely for the disclosure of output buffer and does not fill the gaps of *Alles et al.* mentioned above in § VII. A. 1, in regard to their independent claims.

### **3. Claims 11 and 36 are non-obvious over *Alles et al.* and *Natarajan et al.***

Also meriting reversal are claims 11 and 36, over *Alles et al.* and *Natarajan et al.* The secondary reference, *Natarajan et al.* does not cure the deficiencies of disclosure of *Alles et al.* as detailed above in § VII. A. 1, for their independent claims. Moreover, *Natarajan et al.* does not even manage to disclose the “fault monitor” recited in claims 11 and 36. Rather, the cited passage of *Natarajan et al.* (col. 26:12-26) merely describes an event handler that is “responsible for reporting updated control information stored within data store 252.” There is simply no factual basis for a “fault monitor” necessary to sustain the rejection.

**4. Claims 3, 28, and 50 are non-obvious over *Alles et al.* and *Amara et al.***

Regarding the obviousness rejection of claims 3, 28 and 50 based on *Alles et al.* in view of *Amara et al.*, this rejection should be reversed because *Amara et al.* fails to fill in the gaps of *Alles et al.* For example, *Amara et al.* shows not control interface through which the packet header filter and the forwarding table are programmed.

In addition, the Examiner's proposed modification of *Alles et al.* based on the teachings of *Amara et al.* is improper. Claim 50 recites "a first packet header filter coupled to the first network interface" and "a second packet header filter, different from the first packet header filter, coupled to the second network interface." The packet classifiers 116-120 of *Amara et al.* (col. 4:55-65) operate to classify the packets received at interfaces 102-106 as either internally-destined or external packets. No one of ordinary skill in the art based on this teaching would attempt to modify the switch fabric 340 in the *Alles et al.* to employ multiple "packet header filters" because the proposed modification would result in having multiple sets of "channel identifiers" used for the switch fabric 340. The Examiner's such construction is devoid of any technical merit.

In drawing this conclusion, the Examiner has ignored the basic tenets of obviousness. In rejecting claim under 35 U.S.C. § 103, the Examiner must provide a factual basis to support the obviousness conclusion. *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967); *In re Lunsford*, 357 F.2d 385, 148 USPQ 721 (CCPA 1966); *In re Freed*, 425 F. 2d 785, 165 USPQ 570 (CCPA 1970). Based upon the objective evidence of record, the Examiner is required to make the factual inquiries mandated by *Graham v. John Deere Co.*, 86 S. Ct. 684, 383 U.S. 1, 148 USPQ 459 (1966). The Examiner is also required to explain how and why one having ordinary skill in the art would have been led to modify an applied reference to arrive at the

claimed invention. *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988). In establishing the requisite motivation, it has been consistently held that both the suggestion and the reasonable expectation of success must stem from the prior art itself, as a whole. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *In re Dow Chemical Co.*, 837 F.2d 469, 5 USPQ2d 1529 (Fed. Cir. 1988). None of these requirements have been met for these claims.

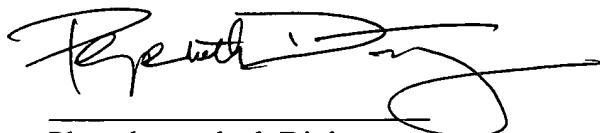
### **VIII. CONCLUSION AND PRAYER FOR RELIEF**

For the foregoing reasons, Appellants request the Honorable Board to reverse each of the Examiner's rejections.

Respectfully Submitted,

DITTHAVONG & MORI, P.C.

9/19/06  
Date



Phouphanomketh Ditthavong  
Attorney for Applicant(s)  
Reg. No. 44658

Stephen C. Carlson  
Reg. No. 39,929

10507 Braddock Rd, Suite A  
Fairfax, VA 22032  
Tel. 703-425-8516  
Fax. 703-425-8518

## **IX. CLAIMS APPENDIX**

1. (Previously Presented) A programmable access device for use in a network access system, said programmable access device comprising:

first and second network interfaces through which packets are communicated with a network;

a packet header filter and a forwarding table, wherein the forwarding table is utilized to forward packets between the first and second network interfaces, and wherein said packet header filter identifies messages received at one of the first and second network interfaces on which policy-based services are to be implemented and passes identified messages via a message interface to an external processor included in said network access system for implementation of the policy-based services by the external processor, wherein said packet header filter passes all other received messages through the packet header filter to an other processor; and

a control interface through which said packet header filter and said forwarding table are programmed.

2. (Original) The programmable access device of Claim 1, wherein the packet header filter receives packets directly from the first network interface.

3. (Original) The programmable access device of Claim 2, wherein the packet header filter is a first packet header filter, and wherein the programmable access device further comprises a second packet header filter that receives packets directly from the second network interface.

4. (Original) The programmable access device of Claim 1, wherein the packet header filter filters packets for service processing based upon protocol information pertaining to protocol layers higher than layer 3.

5. (Original) The programmable access device of Claim 1, and further comprising a policer that polices packets by reference to traffic parameters.

6. (Original) The programmable access device of Claim 5, wherein the policer comprises a marker that marks packets that do not conform with the traffic parameters.

7. (Original) The programmable access device of Claim 1, and further comprising at least a usage monitor that monitors at least one traffic type.

8. (Original) The programmable access device of Claim 7, wherein the usage monitor has an associated threshold that when exceeded generates a reporting event for the usage monitor.

9. (Previously Presented) The programmable access device of Claim 8, and further comprising a reporting interface that communicates the reporting event to the external processor.

10. (Original) The programmable access device of Claim 9, wherein the associated threshold comprises a session activity level threshold.

11. (Original) The programmable access device of Claim 7, and further comprising a fault monitor.

12. (Original) The programmable access device of Claim 1, and further comprising one or more output buffers for outgoing packets.

13. (Original) The programmable access device of Claim 12, and further comprising a scheduler associated with the one or more output buffers that schedules the transmission of outgoing packets within the one or more output buffers.

14. (Original) The programmable access device of Claim 13, wherein the scheduler supports multiple quality of service classes.

15. (Canceled)

16. (Previously Presented) The programmable access device of Claim 1, and further comprising at least a programmable monitor that monitors at least one programmed traffic type.

17. (Previously Presented) The programmable access device of Claim 1, and further comprising a policer that polices packets by reference to programmed traffic parameters.

18. (Previously Presented) The programmable access device of Claim 1, and further comprising one or more output buffers for outgoing packets and an associated scheduler that transmits the outgoing packets from the one or more output buffers through the second network interface according to a programmed methodology.

19. (Original) The programmable access device of Claim 1, wherein the identified message is a session initiation protocol (SIP) message.

20. (Original) The programmable access device of Claim 1, wherein the identified message is an Internet Group Multicast Protocol (IGMP) message.

21. (Original) The programmable access device of Claim 1, wherein the identified message is a Resource Reservation Protocol (RSVP) message.

22. (Original) The programmable access device of Claim 1, and further comprising a plurality of protocol-specific state machines for a respective plurality of protocol types.

23. (Previously Presented) The programmable access device of Claim 22, wherein said plurality of protocol-specific state machines include a transport control protocol (TCP) state machine that, responsive to a control command, provides preferential treatment to a particular TCP session.

24. (Previously Presented) The programmable access device of Claim 1, and further comprising a reporting interface through which the programmable access device reports state information for active sessions to the external processor.

25. (Original) The programmable access device of Claim 24, wherein the reporting interface reports the state information for an active session in response to allocation of service to a new external service controller.

26. (Previously Presented) A method of packet handling in a programmable access device of a network access system, said method comprising:

in response to receiving a series of packets at a first network interface of a programmable access device, filtering the series of packets by a packet header filter at the programmable access device to identify messages upon which policy-based services are to be implemented;

passing identified messages to an external processor included in the network access system for implementation of the policy-based services by the external processor;

for messages that are not identified, routing packets by reference to a forwarding table in the programmable access device and outputting the routed packets at a second network interface of the programmable access device; and

programming the packet header filter and the forwarding table through a control interface of said programmable access device.

27. (Previously Presented) The method of Claim 26, and further comprising receiving packets at the packet header filter directly from the first network interface.

28. (Original) The method of Claim 27, wherein the packet header filter is a first packet header filter, said method further comprising receiving packets at a second packet header filter of the programmable access device directly from the second network interface.

29. (Original) The method of Claim 26, wherein filtering comprises filtering packets for service processing based upon protocol information pertaining to protocol layers higher than layer 3.

30. (Original) The method of Claim 26, and further comprising policing packets by reference to traffic parameters utilizing a policer in the programmable access device.

31. (Original) The method of Claim 30, wherein policing comprises marking packets that do not conform with the traffic parameters.

32. (Previously Presented) The method of Claim 26, wherein the programmable access device includes at least a usage monitor, said method further comprising monitoring at least one traffic type in said series of packets.

33. (Original) The method of Claim 32, wherein the usage monitor has an associated threshold, said method further comprising generating a reporting event for the usage monitor when the threshold is exceeded.

34. (Original) The method of Claim 33, and further comprising communicating the reporting event to an external processor via a reporting interface.

35. (Original) The method of Claim 34, wherein generating a reporting event comprises generating a reporting event in response to a session activity level threshold.

36. (Original) The method of Claim 32, and further comprising monitoring faults utilizing a fault monitor in said programmable access device.

37. (Original) The method of Claim 26, and further comprising buffering outgoing packets in one or more output buffers in said programmable access device.

38. (Original) The method of Claim 37, and further comprising scheduling the transmission of outgoing packets within the one or more output buffers to support multiple quality of service classes.

39. (Canceled)

40. (Previously Presented) The method of Claim 26, wherein the programmable access device further includes at least one programmable monitor, said method further comprising monitoring at least one programmed traffic type utilizing said at least one programmable monitor.

41. (Previously Presented) The method of Claim 26, wherein said programmable access device includes a policer, said method further comprising policing packets by reference to programmed traffic parameters.

42. (Previously Presented) The method of Claim 26, wherein the programmable access device includes one or more output buffers for outgoing packets and an associated scheduler, said method comprising transmitting the outgoing packets from the one or more output buffers through the second network interface according to a programmed methodology.

43. (Original) The method of Claim 26, wherein the identified message is a session initiation protocol (SIP) message.

44. (Original) The method of Claim 26, wherein the identified message is an Internet Group Multicast Protocol (IGMP) message.

45. (Original) The method of Claim 26, wherein the identified message is a Resource Reservation Protocol (RSVP) message.

46. (Original) The method of Claim 26, and further comprising maintaining in said programmable access device a plurality of protocol-specific state machines for a respective plurality of protocol types.

47. (Original) The method of Claim 26, wherein said plurality of protocol-specific state machines include a transport control protocol (TCP) state machine, and wherein the method further

comprises providing preferential treatment to a particular TCP session by said programmable access device in response to a command.

48. (Original) The method of Claim 26, and further comprising reporting state information for active sessions to an external processor via a reporting interface of the programmable access device.

49. (Original) The method of Claim 48, wherein reporting comprises reporting the state information for an active session in response to allocation of service to a new external service controller.

50. (Previously Presented) A device for use in a network access system comprising:  
a first network interface through which packets are communicated with a first network;  
a second network interface through which packets are communicated with a second network;  
a message interface coupled to an external processor that is configured to implement policy-based services;  
a policer configured to discard packets determined as nonconforming to a first traffic parameter;

a first packet header filter coupled to the first network interface and to the message interface, wherein the first packet header filter identifies messages, received from the first network interface, on which policy-based services are to be implemented, wherein the first

packet header filter passes the identified messages to the external processor via the message interface and passes all other messages received from the first network interface to the policer; a marker configured to discard packets determined as nonconforming to a second traffic parameter; a control interface through which said first packet header filter is programmed; and a second packet header filter, different from the first packet header filter, coupled to the second network interface, wherein the second packet header filter identifies messages, received from the second network interface, on which policy-based services are to be implemented, wherein the second packet header filter passes the identified messages to the external processor via the message interface and passes all other messages received from the second network interface to the marker.

**X. EVIDENCE APPENDIX**

Appellants are unaware of any evidence that is required to be submitted in the present Evidence Appendix.

**XI. RELATED PROCEEDINGS APPENDIX**

Appellants are unaware of any related proceedings that are required to be submitted in the present Related Proceedings Appendix.